International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

Extended essay cover

Candidates must complete this page and then give this cover and their final version of the extended essay to their supervisor.

Candidate session number			
Candidate name			
School name			
Examination session (May or November)	MAY	Year	2015

Diploma Programme subject in which this extended essay is registered: COMPUTER SCIENCE

(For an extended essay in the area of languages, state the language and whether it is group 1 or group 2.)

Title of the extended essay: With the rapid increase in web social interaction, is there a reliable cipher algorithm that would allow people to communicate electronically without worries of deceit and deception?

Candidate's declaration

This declaration must be signed by the candidate; otherwise a mark of zero will be issued.

The extended essay I am submitting is my own work (apart from guidance allowed by the International Baccalaureate).

I have acknowledged each use of the words, graphics or ideas of another person, whether written, oral or visual.

I am aware that the word limit for all extended essays is 4000 words and that examiners are not required to read beyond this limit.

This is the final version of my extended essay.

Candidate's signature: _____ Date: 5/2/2015

Supervisor's report and declaration

The supervisor must complete this report, sign the declaration and then give the final version of the extended essay, with this cover attached, to the Diploma Programme coordinator.

Name of supervisor (CAPITAL letters)

Please comment, as appropriate, on the candidate's performance, the context in which the candidate undertook the research for the extended essay, any difficulties encountered and how these were overcome (see page 13 of the extended essay guide). The concluding interview (viva voce) may provide useful information. These comments can help the examiner award a level for criterion K (holistic judgment). Do not comment on any adverse personal circumstances that may have affected the candidate. If the amount of time spent with the candidate was zero, you must explain this, in particular how it was then possible to authenticate the essay as the candidate's own work. You may attach an additional sheet if there is insufficient space here.

has been deeply interested in the algorithms of cryptography. He made an earnest effort to analyse strengths and weaknesses of those and further reason and suggest an ideal hybrid combination of symmetric & asymetric. He was excellent in terms of attempting all necessary required criterions of the essay and good with deadlines too. The analysis is original and appropriate citations & references have been made.

This declaration must be signed by the supervisor; otherwise a mark of zero will be issued.

I have read the final version of the extended essay that will be submitted to the examiner.

To the best of my knowledge, the extended essay is the authentic work of the candidate.

As per the section entitled "Responsibilities of the Supervisor" in the EE guide, the recommended number of hours spent with candidates is between 3 and 5 hours. Schools will be contacted when the number of hours is left blank, or where 0 hours are stated and there lacks an explanation. Schools will also be contacted in the event that number of hours spent is significantly excessive compared to the recommendation.

I spent [4.5] hours with the candidate discussing the progress of the extended essay.

Supervisor's signature: _____ Date: 5 Feb 2015

Assessment form (for examiner use only)

Candidate session number					

Criteria	Achievement level				
	Examiner 1	maximum	Examiner 2	maximum	Examiner 3
A research question	1	2		2	
B introduction	1	2		2	
C investigation	2	4		4	
D knowledge and understanding	2	4		4	
E reasoned argument	2	4		4	
F analysis and evaluation	2	4		4	
G use of subject language	2	4		4	
H conclusion	1	2		2	
I formal presentation	2	4		4	
J abstract	1	2		2	
K holistic judgment	2	4		4	
Total out of 36	18				

ame of examiner 1: _____ Examiner number: _____
APITAL letters)

ame of examiner 2: _____ Examiner number: _____
APITAL letters)

ame of examiner 3: _____ Examiner number: _____
APITAL letters)

IB Assessment Centre use only: **B:** _____

IB Assessment Centre use only: **A:** _____

WITH THE RAPID INCREASE IN WEB SOCIAL INTERACTION, IS THERE A RELIABLE CIPHER ALGORITHM THAT WOULD ALLOW PEOPLE TO COMMUNICATE ELECTRONICALLY WITH THE SAME CONFIDENCE FOUND IN THE PHYSICAL WORLD WITHOUT WORRIES OF DECEIT AND DECEPTION?

Approach: Investigation and mathematical analysis of symmetric and asymmetric encryption algorithms. Further, looking at the possibility of combining the strengths of the two to generate a reliable and efficient cipher.

Word count: 3790

CONTENTS:

poorly set-out I -

Acknowledgements

I would like to thank my extended essay supervisor, who has guided and supported me throughout this extended essay journey.

I would also like to thank our IB coordinator, , for organizing and scheduling all the extended essay meetings and also, for encouraging me throughout.

As it is a big topic

ABSTRACT

My extended essay will be the result of my investigation into the two different modes, namely- symmetric and asymmetric encryption and decryption of the data which transfers through networks. The leading question for the study was "**WITH THE RAPID INCREASE IN WEB SOCIAL INTERACTION, IS THERE A RELIABLE CIPHER ALGORITHM THAT WOULD ALLOW PEOPLE TO COMMUNICATE ELECTRONICALLY WITH THE SAME CONFIDENCE FOUND IN THE PHYSICAL WORLD WITHOUT WORRIES OF DECEIT AND DECEPTION?**"

RQ ✓

My approach to attempt an answer to the above has been analyzing the two different types of cryptography. A thorough analysis of both symmetric and as asymmetric cryptography would help me to arrive at a useful comparison.

This would also help me to validate my thought whether a combination between the two would be possible and useful.

Mathematics is done in both symmetric and asymmetric methods of encryption and decryption and a brief analysis is stated after every operation. I have chosen a piece of data and have applied both the methods to encrypt and decrypt the data. I would also explore the possibility of a hybrid cryptography model that uses the strengths of both the methods. For approaching symmetric encryption, I looked at block ciphers and stream ciphers and the algorithm used to encrypt the data. For asymmetric encryption, I looked at the Diffie and Hellman algorithm and the RSA algorithm to understand the mathematics behind the asymmetric cryptography. Thereafter, I introspected if advancements such as Moore's Law threaten the reliability of such asymmetric cryptosystems.

met ✓

The analysis presented as part of this essay would hopefully succeed in creating a bias in the mind of the reader about the ideology about combining the two and developing a hybrid cryptography model.

Concl ?

WORD COUNT- 282

conclusion is quite vague

J31

1. Methodology of Investigation

The aim of this research paper is to evaluate the viability of symmetric encryption and then compare with asymmetric encryption using a sample data and investigating the mathematics behind the algorithms in each case.

Further, to explore the viability and possibility of utilizing features of both methods to be able to arrive at an ideal method of encryption.

2.Introduction:

Secrecy has been in use from the time of Caesar in the Roman Empire and is still in use in the cyber world of networking and communication. Effective wars have been fought using this method of "**hiding secrets**" using strategic plans within war zones.

In today's cyber world, we use a method of preserving security and secrecy of information known as **Cryptography**.

CRYPTOGRAPHY:

What is cryptography in the cyber world? How different or similar it is to the Caesar's way of "**hiding secrets**. The essay attempts to first describe the term cryptography and then introspect various algorithms through which we can "**hide secrets**" in the cyber world.

"I am fairly familiar [1]with all forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyze one hundred and sixty separate ciphers", said Holmes.

The word cryptography or cryptology implies the study of hidden secrets. There are two main types of cryptography techniques that are and were used in different times. These are **Symmetric and Asymmetric** cryptography.

For a smooth flow of understanding about the topic. We need to know a few key terms.

-The original message which has to be kept secret is known as the **plain text**.

-The algorithm needed to convert the plain text in to the secret message will be defined as the **encryption algorithm**.

- To execute the encryption algorithm which is kept of a lock, we would need a **secret key** to lock it. The encryption algorithm encrypts or convert the **plain text** into **cipher text.**

[1] These lines are quote from the book "The Adventure of the dancing men"

-**Cipher text** is the coded message which will be transmitted to the decryption part of the receiver's part.

-The cipher text has to be converted into plain text in order to get the message. This is done by using the key in the **Decryption algorithm**.

flowchart ?

Classical encryption techniques:

Caesar cipher:

Under this category, swapping of alphabets takes place. Such as, the 3rd alphabet with the first one. Alphabetical wrapstake place so that first A is replaced with D and so on. When Z is reached the alphabets get reset to A

Let us encrypt a message: "HEY I AM A GENIUS" (PLAIN TEXT)

H-k, E-H, Y-B, I-L, A-D, M-P, A-D, G-J, E-H, N-Q, I-L, U-X, S-V

Cipher text- KHB L DP D JHQLXV

Here, the key is assumed to be 'K' and the value of k is 3. ? - the letter "K" ??

K can take any whole number value. It is only known to the sender and the receiver who are communicating.

We can also assume the alphabets to be numbers and form a mathematical expression. Such as A=1, B=2 and so on.

Therefore, the expression for encryption would be

C= E (P) = (P+K-1) MOD 26+1

← decryption

P= D (C) = (C-K+25) MOD 26 +1

Here, C- CIPHER, P- PLAIN TEXT, D-DECRYPTION ALGORITHM, E-ENCRPYTION ALGORITHM.

But if the intruder who wants to decrypt the message without the permission of the sender can try out different security attacks such as brute force attacks or he can also try out all the 25 possible keys. Brute force attack is lengthy and can be exhaustive method of permutation and substitution if the key is a large value.

This particular cipher was effective during the tenure of Caesar! Nowadays it is child's play to decrypt the cipher and obtain the original message by reversing the method of encryption.

I hope to explore in the body of this essay, other ciphers and methods of encryption the hope to be able to successfully arrive at the strengths and weaknesses of symmetric cryptography and of the same to the maximum. How we can reap the benefits?

MONO-ALPHABETIC Cipher:

Here the key is generated through arbitrary substitution. The alphabets are arranged by any order such as A can be replaced as R and so on.

Therefore, the key which is created by the permutation of the alphabets tells us the way to decrypt the cipher text.

The key can look like: "ZAQWSXCDERFVBGTYHNMJUIKLOP"

There can be 26! Or 4X1024 keys possible.

So how does this key work?

But in this type of cipher also, guesses can be made by observing the relative frequency of letter, diagrams in the text. Although, these guesses are not made by human brain. The brute force attack is done by computers and it is also a time consuming process.

The original RQ deals with the security of "web social interaction" - there is no mention of this in the RQ!

3.INVESTIGATION

Investigating the cipher strength using symmetric cryptographic technique:

Here, after explaining about the block and stream ciphers I will investigate the DES algorithm which has been in use for a very long period.

In symmetric encryption, only a single key is used for both encryption and decryption of data. This is done by cipher system of encryption and decryption. There are two types of cipher systems we will follow: Block cipher and stream cipher system. These systems are the traditional way to encrypt the data. The importance to know about these methods is to understand the DES (data encryption standard) easily. Otherwise, it gets really difficult to understand the algorithms used in the DES method of encryption.

What is the DES?

So first we will be drawing a comparison between the block cipher and stream cipher structures.

Stream cipher: It encrypts a digital data stream one bit or byte one by one. The plain text bit stream (p_i) is matched. A Vernam cipher in which k_i and p_i are equal will be used as a one-time pad version. This cipher will be unbreakable unless and until this k_i is somehow acquired. However, k_i must be available in advance for this to happen with both the sender and receiver through some means may be an independent and secure channel.

What's this?

A general example for the bit stream can be "1010101101001" which is a plain text and the stream cipher is of the same length but with the permuted pattern.

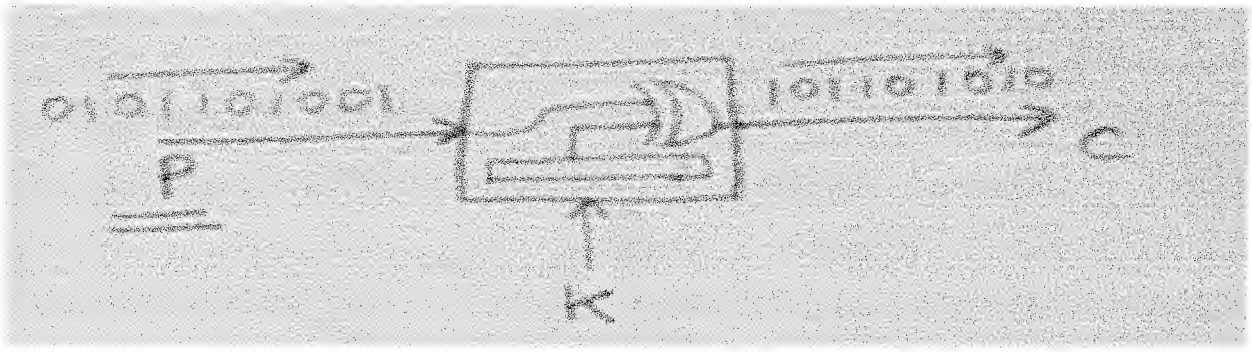
These kind of ciphers are proved to be useful when the communication has to be amongst the stations, in the satellites and where the continuous speech encryption has to be done. Such as when you have to talk to an astronaut from a Nasa space station and the message has to be cofidential. Stream cipher would be handy to encrpyt the message simultaneously and transmit to the astronaut.

??

This hasn't been well-explained.

Inconsistent formatting I

a lot of information is being presented but the essays looks clarity & coherance at the moment



BLOCK CIPHER: A block cipher is in which the plain text is treated as a block and is used to produce the cipher text block of the same length. The typical size of the block is 64 bit to 128 bits.

If there are 'n' bits in a plain text block then a cipher text of 'n' bits will be produced after a block cipher operates on a plaintext block. The number of different blocks possible will be 2^n therefore, for decryption each cipher block must again be unique. This transformation is reversible. Hence, called reversible mapping.

REVERSIBLE MAPPING

PLAIN TEXT	CIPHER TEXT
00	11
01	10
10	00
11	01

Here, for simplicity we are working in binary digits to understand the method in a swift way.

I will be using these ciphers to learn about the DES algorithm in detail and efficiently. These ciphers are the building blocks to the DES encryption technique. If we talk about symmetric encryption, DES encryption is the most widely used encryption technique and is really fast.

DES (Data encryption standard) and the existence of multiple times DES

- The block size of the cipher is 64-bit
- The size of the key is 56 bits.

The algorithm can be shown diagrammatically.

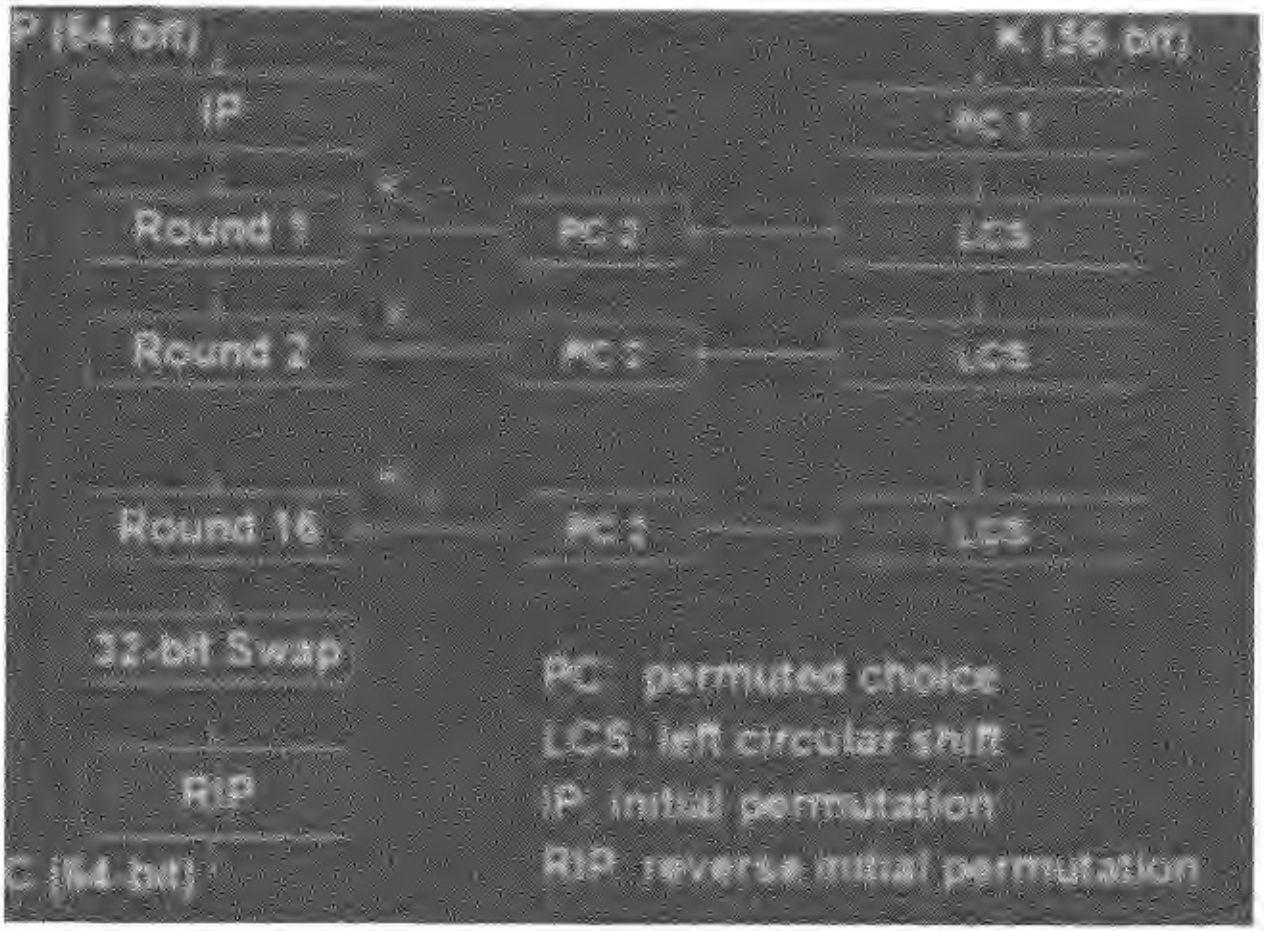


Fig1[2]

Here, the encryption and decryption takes place in 16 rounds.

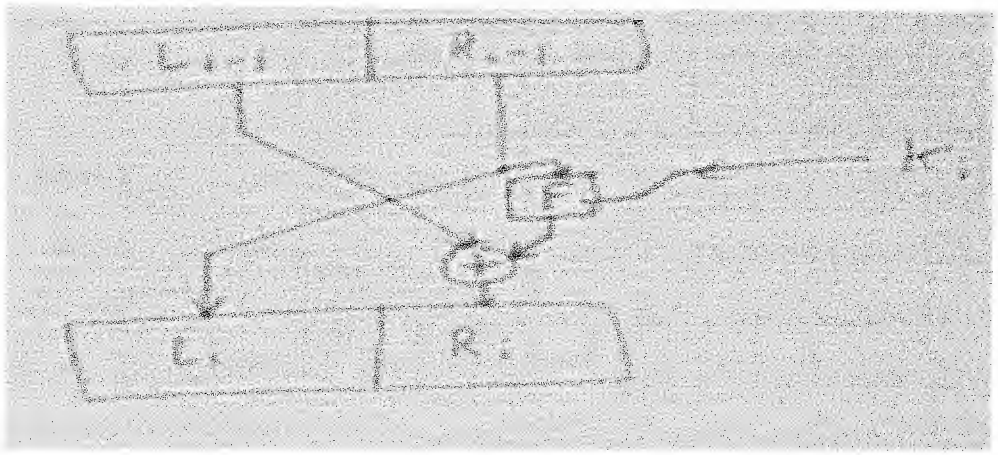
The 64- bit plain text would be going through initial permutation first and then the rounds are initiated. The keys are generated and are defined as k1, K2 and k3.

This explained clearly what happens in the rounds during the cryptographic process.

$L_I = R_{I-1}$

$R_i = L_{i-1}$ XOR F (R_{I-1}, K_i)

[2]"The Caesar Cipher." *Khan Academy*. N.p., n.d. Web. 16 Jan. 2015.



This is can be also be decrypted by the intruders by brute force technique as it is a 56-bit key and if the intruder has a fast processing computer, the brute force would be a child's play.

This was a disappointment for me as I was expecting a strong cipher from the DES algorithm. Although if the DES algorithm is repeated multiple times* the cipher can be made strong. But it consumes time and is also an exhaustive method.

**multiple time DES is known as TRIPLE DES ALGORITHM.*

DES*[3] *algorithm has been in use for a very long time so a new algorithm was needed. The triple DES algorithm is although effective but is slow to execute. So this was calling a newer and stronger way of encryption.

Merits and demerits of symmetric cryptography:

- MERITS:
  1. Extremely secure, if the key length crosses the 56bit key length such as 128 bit key or the 256 bit key length. The cipher becomes extremely secure and complex to be broken by any cryptanalyst*. (*he is a person who can attempt a brute force attack to decrypt the cipher and get the information from the plain text.)
  2. Relatively fast, the symmetric cryptography doesn't include complex mathematics. It is easy going to do the encryption and decryption process.

- Demerits:
  1. **Sharing the key**, the problem comes when both the parties have to share the key. The key has to be transferred to the 2nd party so that it can decrypt the cipher and obtain the plain text. But this key is vulnerable to the intruders and they can perform various cyber-attacks to get the key.
  2. **Data can be compromised:** Once the intruder has his hands on the key, data from both the sides can be compromised.

[3] Data encryption standard

The journey of searching a strong encryption technique led me to public key crypto systems.

Public- key systems are described by the use of a cryptic algorithm which is coated with two keys, one of these keys is a private key and the other is the public key. It generally depends on the application, which will be the private key and which will be the public key. In this case the sender has the provision of using either his private key or the receiver's public key, or both, to perform some type of cryptographic process. We can describe public key cryptosystems into three categories:

- **Encryption/decryption**: The sender creates the encrypted message with the other user's public key.
- **Digital signatures:** The sender "signs" the message with its private key. Signing is achieved by a cryptographic algorithm applied to the message that is a function of the message.
- **Key exchange:** Two sides of the end-user devices cooperate to exchange a session key.

Some algorithms are suitable for all the three applications mentioned above, whereas others can be used only for one or two of these applications.

REQUIREMENTS FOR PUBLIC KEY CRYPTOGRAPHY:

Diffie and Hellman [4]postulated this system without demonstrating that such algorithms exist. However, they gave a layout for the conditions that such algorithms must fulfill. These made up a set of conditions which were known as DIFF76b.

1. "It is computationally for an end- user device B to generate a pair of public keys and private keys (PU_b, PR_b).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M , to generate the corresponding cipher text:
   $C= E (PU_b, M)$
   Where C stands for cipher text (the encrypted text), E (encryption), M (message).
3. It is computationally easy for the receiver B to decrypt the resulting cipher text using the private key to recover the original message.
   $M= D (PR_b, C) = D [PR_b, E (PU_b, M)$
4. It is computationally infeasible for an adversary, knowing the public key, $PU_b$to determine the private key, PR_b
5. It is computationally infeasible for an adversary, knowing the public key, PU_b, and a cipher text, C, to recover the original message which is M.
6. The two keys are applied in either order:
   $M= D [PU_b, E (PR_b, M) = D [PR_b, E (PU_b, M)]$"

[4] Diffie and Hellman postulates are taken from the book 'Network and security by William Stallings'.

These were the requirements or we can say standard conditions for the generation for the public – key cryptosystems.
The requirements lead to the use for a trap-door one-way function. A **one-way function** is a function that converts a domain into a range such that every function value has a unique inverse, so that the calculation of the inverse is possible.

Y= f(X) easy
X= f^{-1}(Y) infeasible

The trap door one way function is easy to calculate in one direction and possible to calculate in other direction if and only if certain additional information is known. In that case this calculation will be possible in polynomial time. We can summarize as follows: A trap- door- one – way function is a family of invertible functions f_k, such that
If k and X are both known then Y= f_k(X) and also X= f_k^{-1} (Y) {if X and k are known) are both easy, however, when k and Y are known X= f_k^{-1} (Y) will not possible, if Y is known but k is not known.

Thus, the development of a practical public- key scheme depends on discovery of a suitable trap-door one-way function.

Encryption

Let's assume Mr. A wishes to communicate with Mr. B through an encrypted message. A public key(x,y) gets transmitted along with the message to Mr. B but a private key Z remains secret. Now, when Mr. B wishes to reciprocate a message MSG to Mr. A then MSG will first be converted to an integer 'm' such that $0 \leq m < x$ by using a protocol that would prevent the use of predictability to find cribs to decipher the message. Further, a cipher text is created corresponding to,

$$C \equiv m^y (mod\ x)$$

This process is swift and uses exponentiation by squaring. Mr. Bfinally transmits *c (cipher)* to Mr. A.

How do we decrypt the encrypted message?

Decryption

Mr. A can recover *m* from *c* by using the private key exponent *d* via computing

$$m \equiv c^z (mod\ x)$$

Given m, Mr. A can recover the original message *MSG* by reversing the protocol set by the padding scheme.

A worked example

The following example of RSA encryption and decryption uses OPEN secure socket layer and generates a real key pair as shown below.

The objective is to be able to generate the real key pair and this is done through OPEN SSL. Two distinct prime numbers are taken Let us say, these numbers are 'p' and 'q'. The product is denoted by 'n'.The quotient of the product is denoted by φ

$p = 83$ And $q = 53$

1. Calculate $n = pq$ giving

$$x = 83 \times 53$$

2. Compute the quotient of the product as $\varphi(n) = (p - 1)(q - 1)$ giving

$$\varphi(4399) = (83 - 1)(53 - 1) = 4264$$

3. Choose any number $1 < e < 3828$ that is co-prime to 4264. Choosing a prime number for e leaves us only to check that e is not a divisor of 4264.

Let $e = 17$

4. Compute d, the modular multiplicative inverse of e (mod $\varphi(n)$) yielding

$$d = 1505$$

The **public key** is (x = 4399, y = 17). For a padded plaintext message m, the encryption function is

$$c(m) = m^{17} mod\ 4399$$

The **private key** is (n = 4264, d = 1505). For an encrypted cipher text c, the decryption function is

$$m(c) = c^{1505}\ mod\ 4399$$

For instance, in order to encrypt m = 65, we calculate

$$c = 65^{17}\ mod\ 4399 = 253$$

To decrypt c = 2790, we calculate

$$m = 253^2\ mod\ 4399 = 2423$$

This process of generating a strong public key seems lengthy.

Of course, now with the application of Moore's Law and even if one looks at processing in qubits as done in Quantum computers one can safely assume that this processing would be much faster and generating these keys would probably be much quicker.

Further the speed of calculation can be increased by using the modulus of factors as in the '**Chinese remainder theorem** ' (mod $p*q$ using mod p and mod q).

The values d_p, d_q and q_{inv}, which are part of the private key are computed as follows:

D_p= d mod (p – 1) = 1505 mod (83– 1) = 29

$D_{p=}$ d mod (q – 1) = 1505 mod (53– 1) = 49

$Q_{inv} = q^{\wedge} -$ 1mod p = 53 ^-1 mod 83 = 47

⇨ (q_{inv}X q) mod p = 47 X 53 mod 83 = 1

Here is how d_p, d_q and q_{inv} are used for efficient decryption. (Encryption is efficient by choice of public exponent e)

M_1 = c^$d_p$mod p = 1505^29 mod 83 = 66

M_2 = c^$d_q$mod q = 1505^49 mod 53 = 2

H= (q_{inv}X ($m_1 - m_2$)) mod p = (47 X 64) mod 67 = 1

M= m_2 + h x q = 2 + 1 x 66 = 198

Asymmetric cryptography has merits and demerits:

- Merits:
  1. The cryptosystem involves 2 layer encryption. Once it is done from the private key and 2nd time it is done with the public key or vice versa.
  2. The level of security increases in this cryptosystem as the encryption and decryption has to be done with a pair of keys. One with a public key and other with a private key. The algorithms can be executed with any of the keys.
  3. This particular behavior of exchange of keys allows a secure transmission.

- Demerits:

1. The asymmetric cryptography is a slow process.
2. If the key is a large number then the exponential process to generate the cipher text becomes really exhausting. On a contrary we need to maintain the length of the key in order to maintain the high level of security.

Further ,**Moore's Law**[5]states that the relation between the number of transistors per square inch and the year of introduction are related linearly as they double each year.So computers will process at a much faster rate and therefore private keys will take less time to crack. Further, quantum computers that work on qubits as against the classical binary system could easily break a large number into factors making it necessary to devise a more effective encryption method.It seems plausible to combine strengths of different crypto algorithms to achieve this to a reasonable degree.

Hybrid cryptography:

Cryptanalyst tend to develop a mentality of hacking either of the cryptic systems.

So, if the strengths of both the symmetric and asymmetric cryptic systems are combined into a hybrid model that adds another dimension. Pertaining to higher security as the complexity of the asymmetric and the speed of the symmetric cryptography may be harnessed.This particular type of cryptosystem can overcome the demerits in both asymmetric and symmetric cryptosystems.

My idea is to follow the normal symmetric way of encrypting the plain text. But the key should be encrypted asymmetrically.

The key goes through 2 layer encryption with the private and public key.

Now, I would be explaining my particular idea of combining these two cryptic methods.

Let the plain text be – "hello good morning"

I will be encrypting the plain text with the transposition cipher.

I select the key size to be 5 letters

Therefore,

Key	1	5	2	3	4
	H	E	L	L	O
	G	O	O	D	M
	O	R	N	I	N
	G				

Now, I will write the letter column-wise to generate the cipher:

CIPHER: HGOG LON LDI OMN EOR

[5] Gordon Moore, 1965,Co-Founder of Intel

Now, that I have used the symmetric method to encrypt the plain text. I would be using the key which consists of 5 letters with asymmetric encryption method.

For the asymmetric method, I need to generate another key which can be regarded as the private key.

Let the private key consist of 7 letters.

Therefore, my two prime numbers here are 5 and 7.

Let,

$$p = 5 \; and \; q = 7$$

$$n = p \times q = 5 \times 7 = 35$$

$$\varphi(n) = (p-1)(q-1) = (5-1)(7-1) = 4 \times 6 = 24$$

Now, selecting an integer 'e'- $GCD\{\varphi(n), e\} = 1; 1 < e < \varphi(n)$
Therefore, the integer can be assumed as 17.

Now, we calculate 'd' – $d = (e\text{^} - 1) \text{mod } \varphi(n) = \frac{1}{17} \times mod24$
Or $d \times e = 1 \text{mod} 24$
Therefore,
D= can be equal to 23.

Therefore my public and private key for the process would be,
KU (17, 35) - PK
KR (23, 35) – Private Key

Therefore if M= 5
Where m= message (in my case the key of the symmetrically encrypted message)
Cipher text : 5^5(mod35)
= 3125(mod35)
=10

Decryption process=
M= 10^23(mod35)
=15

Finally, the lesson learned is that successful encryption of the key with the asymmetric algorithm may be carried out. Further, the plain text can be encrypted with this encrypted

key. This brings on the 4- layer encrypted message including the high level of security and quick speed of encryption.
Good encryption parameters must be non - malicious. This preference of symmetric cryptography over asymmetric cryptography is based on the idea that asymmetric cryptography uses parameterized mathematical objects and I suspect that such parameters could be specially chosen to make the system weak. A 4 layered encryption technique as explained above should do the trick and promise security to a large extent.

Conclusion

On the basis of this investigation, it is possible to have a clear standing on "With the rapid increase in the interaction of people electronically, is there a reliable cipher algorithm that would allow people to communicate electronically with the same confidence found in the physical world without worries of deceit and deception?".
Through this in depth mathematical analysis of the algorithms of various encryption techniques, the strengths and weaknesses of each system can be drawn out and this helps in adding value to the research question.
Symmetric encryption has been widely used and implemented for a long while for communicating over a network.
The main limiting factor of the same was the level of complexity is very low which provides lesser security in comparison to the asymmetric cryptography.
Asymmetric cryptography came as an amendment to the above and promised greater security.
However, for the same key size typically the asymmetric encryption is less secure. In the real world, one can take care of this by using larger keys
More secure is generally an unmeasurable quantity. Resistance of a message M to attack X by threat Y is much more meaningful.
It appears that the asymmetric part is often just used for the key exchange and then the actual data is encrypted with a symmetric algorithm.
In my opinion, the answer to the problem seems to be floating in between the two techniques. A 4- layer encryption as explained on a message will contribute towards high level of security and quick speed of encryption.

Evaluation

Having taken my own stand bending toward the hybrid algorithm. Given more time, an in-depth exploration into algorithms of symmetric hill cipher, blowfishas well as digital signature algorithm of asymmetric and crypto algorithms like Shor's used in Quantum computers would further strengthen or affect my convictio

1 WORKS CITED

BOOK

1. 'NETWORK AND SECUIRITY ', BY WILLIAM STALINGS (BOOK)- **CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE**

Author: William Stallings

Publication:

Book

Cryptography and Network Security: Principles and Practice

5th

WEBSITES

"Hundreds of Free Online Tools and Calculators." *MiniWebtool*. N.p., n.d. Web. 16 Jan. 2015. <http://www.miniwebtool.com/>.

"1000+ Free Courses, 25000+ Video Lectures from 30+ Universities on 35+ Subjects." *Free Video Lectures, Video Tutorials and Online Video Courses*. N.p., n.d. Web. 15 Jan. 2015.freevideolectures.com

"Schneier on Security." *Blog*. N.p., n.d. Web. 16 Jan. 2015. <http://www.schneier.com/blowfish.html>.

"The Caesar Cipher." *Khan Academy*. N.p., n.d. Web. 16 Jan. 2015. <http://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher>.PPT – Block Ciphers and Data Encryption Standard DES PowerPoint presentation | free to download

"What Is Hybrid Encryption? - Definition from Techopedia." *Techopedias*. N.p., n.d. Web. 16 Jan. 2015. <http://www.techopedia.com/definition/1779/hybrid-encryption>.www.khanacademy.org/XOR exploration | Ciphers | Khan Academy

"Modular Arithmetic." -- *from Wolfram MathWorld.* N.p., n.d. Web. 15 Jan. 2015. <http://mathworld.wolfram.com/ModularArithmetic.html>.

"Asymmetric Cryptography." *What Is ?* N.p., n.d. Web. 16 Jan. 2015. <http://searchsecurity.techtarget.com/definition/asymmetric-cryptography>.

"Randomized Algorithms." *MIT OpenCourseWare*. N.p., n.d. Web. 16 Jan. 2015. <http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-856j-randomized-algorithms-fall-2002/index.htm>.

The whole essay is quite confusing with terms & ideas introduced without much (if any) explanation.
Analysis is limited & the student's own understanding does not shine through.
The idea of a "hybrid" model is, of course, the basis of SSH/THS.
Presentation is inconsistent & some diagrams are of poor quality

The original RQ was based on "web social interaction", but this was never mentioned again.